

and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for investigative purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants.

(u) ID: GNSA 28 (General Exemption)

(1) *System name:* Freedom of Information Act, Privacy Act and Mandatory Declassification Review Records.

(2) *Exemption:* During the processing of letters and other correspondence to the National Security Agency/Central Security Service, exempt materials from other systems of records may in turn become part of the case record in this system. To the extent that copies of exempt records from those “other” systems of records are entered into this system, the National Security Agency/Central Security Service hereby claims the same exemptions for the records from those “other” systems that are entered into this system, as claimed

for the original primary system of which they are a part.

(3) *Authority:* 5 U.S.C. 552a(k)(2) through (k)(7).

(4) *Reasons:* During the course of a FOIA/Privacy Act and/or MDR action, exempt materials from other system of records may become part of the case records in this system of records. To the extent that copies of exempt records from those other systems of records are entered into these case records, NSA/CSS hereby claims the same exemptions for the records as claimed in the original primary system of records of which they are a part. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

[68 FR 28757, May 27, 2003, as amended at 69 FR 62408, Oct. 26, 2004; 74 FR 55779 and 55780, Oct. 29, 2009; 76 FR 22615, 22616, Apr. 22, 2011; 77 FR 15596, 15597, Mar. 16, 2012; 77 FR 19095, Mar. 30, 2012]

PART 323—DEFENSE LOGISTICS AGENCY PRIVACY PROGRAM

Sec.

323.1 Purpose.

323.2 Applicability.

323.3 Policy.

323.4 Responsibilities.

323.5 Access to systems of records information.

323.6 Exemption rules.

AUTHORITY: Privacy Act of 1974, Pub. L. 93-579, Stat. 1896 (5 U.S.C. 552a).

SOURCE: 78 FR 25854, May 3, 2013, unless otherwise noted.

§ 323.1 Purpose.

This part sets out Defense Logistics Agency policy, assigns responsibilities, and prescribes procedures for the effective administration of the DLA Privacy Program.

§ 323.2 Applicability.

This part:

(a) Applies to Defense Logistics Agency Headquarters (DLA HQ) and all other organizational entities within the Defense Logistics Agency (hereafter referred to as “DLA Components”).

(b) Shall be made applicable by contract or other legally binding action to

§ 323.3

32 CFR Ch. I (7–1–13 Edition)

U.S. Government contractors whenever a DLA contract requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records on behalf of DLA.

§ 323.3 Policy.

DLA adopts and supplements the DoD Privacy Program policy and procedures codified at 32 CFR 310.4 through 310.53, and appendices A through H of 32 CFR part 310.

§ 323.4 Responsibilities.

(a) *General Counsel.* The General Counsel, DLA, under the authority of the Director, Defense Logistics Agency:

(1) Implements the DLA Privacy Program and is hereby designated as the Component Senior Official for Privacy.

(2) Serves as the DLA Final Denial Appellate Authority.

(3) Provides advice and assistance on all legal matters arising out of, or incident to, the implementation and administration of the DLA Privacy Program.

(4) Serves as the DLA focal point on Privacy Act litigation with the Department of Justice; and will advise the Defense Privacy and Civil Liberties Office on the status of DLA privacy litigation. This responsibility may be delegated.

(5) Serves as a member of the Defense Privacy Board Legal Committee. This responsibility may be delegated.

(6) Supervises and administers the DLA FOIA and Privacy Act Office (DGA) and assigned staff. This responsibility may be delegated.

(7) May exempt DLA systems of records.

(b) *Initial Denial Authority (IDA) at Headquarters DLA.* By this part, the DLA Director designates the Head of each Headquarters DLA Component as an IDA. Each Head may further delegate this responsibility to their Deputy. For the DLA General Counsel's Office, the Deputy General Counsel shall serve as the Initial Denial Authority (IDA).

(c) *DLA Privacy Act Office.* The DLA Privacy Act Office (DGA) staff:

(1) Formulates policies, procedures, and standards necessary for a uniform DLA Privacy Program.

(2) Serves as the DLA representative on the Defense Privacy Board and the Defense Data Integrity Board.

(3) Provides advice and assistance on privacy matters.

(4) Develops or compiles the rules, notices, and reports required under 32 CFR part 310.

(5) Assesses the impact of technology on the privacy of personal information.

(6) Conducts Privacy training for personnel assigned, employed, and detailed, including contractor personnel and individuals having primary responsibility for implementing the DLA Privacy Program.

(7) Develops forms used within the DLA Privacy Program. This part serves as the prescribing document for forms developed for the DLA Privacy Program.

(d) *DLA Components Heads.* The DLA Components Heads:

(1) Designate an individual as the point of contact for Privacy matters for their DLA Component and advise DGA of the name of official so designated. This individual also will serve as the Privacy Officer for the co-located tenant DLA organizations.

(2) Designate an official to serve as the initial denial authority for initial requests for access to an individual's records or amendments to records, and will advise DGA of the names of the officials so designated.

(e) *DLA Acquisition Management Directorate (J-7).* The DLA Acquisition Management Directorate (J-7) shall be responsible for:

(1) Developing the specific DLA policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to 32 CFR 310.12.

(2) Establishing an appropriate contract surveillance program to ensure contractors comply with the procedures established in accordance with 32 CFR 310.12.

§ 323.5 Access to systems of records information.

(a) Individuals who wish to gain access to records contained in a system